

CLAIMS

What is claimed is:

1. A computer system, comprising:
 - a chipset;
 - a bus coupled to the chipset to communicate a trusted data cycle to an internal component of the computer system; and
 - a circuit coupled to the bus that prevents a device external to the computer system from accessing the trusted data cycle.
2. The computer system of claim 1, wherein the bus is a Low Pin Count bus.
3. The computer system of claim 1, wherein the component provides protected memory storage.
4. The computer system of claim 1, wherein the component provides platform authentication.
5. The computer system of claim 1, wherein the component maintains a protected path between the chipset and a keyboard.
6. The computer system of claim 1, wherein the computer system is a notebook computer.
7. A circuit, comprising:
 - means for transmitting data on a Low Pin Count (LPC) bus; and
 - means for preventing trusted data cycles on the Low Pin Count (LPC) bus from being accessed by an unauthorized component.
8. The circuit of claim 7, further comprising:

means for connecting an external device to a notebook computer.

9. The circuit of claim 7, further comprising:

means for monitoring data cycles on the LPC bus.

10. A method, comprising:

monitoring a chipset of a computer system for communication of trusted data cycles on a bus; and

preventing the trusted data cycles from being available to a component external to the computer system.

11. The method of claim 10, wherein trusted data cycles begin with a "0101" value.

12. The method of claim 10, further comprising:

communicating trusted data cycles between the chipset and a first component.

13. The method of claim 12, wherein the communication between the chipset and the first component is in plaintext format.

14. The method of claim 10, further comprising:

communicating trusted data cycles between the chipset and a second component.

15. The method of claim 14, wherein the communication between the chipset and the second component is in plaintext format.

16. The method of claim 15, wherein the second component maintains a

protected path between the chipset and a keyboard, wherein keystroke data is communicated by the chipset to protected memory and trusted applications.

17. The method of claim 15, wherein the second component maintains a protected path between the chipset and a mouse, wherein pointer data from the mouse is communicated by the chipset to protected memory and trusted applications.

18. The method of claim 12, wherein the first component protects secret data of the computer system by encrypting the secret data.

19. The method of claim 18, wherein the secret data is decrypted by hardware of the computer system.

20. The method of claim 18, wherein the first component merges data with the computer system's configuration values.

21. The method of claim 18, wherein the first component requests for a system identification request.

22. The method of claim 21, wherein a trusted third party chip verifies the computer system's identification and sends a response to the first component.